risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 22/09/2025
Aceitação/Acceptance: 13/11/2025

Madurez en ciberseguridad y resiliencia digital en PYMEs iberoamericanas: diagnóstico y desafíos estratégicos

Hernán Cornejo

mghcornejo@gmail.com

[1] Universidad Tecnológica Nacional, Zeballos 1341, 2000, Rosario, Argentina.

DOI: 10.17013/risti.60.127–141

Resumen: Este artículo analiza el nivel de madurez en ciberseguridad y resiliencia digital de las pequeñas y medianas empresas (PYMEs) iberoamericanas, un sector especialmente vulnerable ante el aumento de ciberamenazas globales. A partir de un enfoque exploratorio-descriptivo, se propone un modelo de diagnóstico basado en el marco NIST Cybersecurity Framework, complementado con indicadores de gestión organizativa y cultura de seguridad. Los resultados evidencian brechas significativas en la adopción de políticas formales, formación del personal y continuidad operativa ante incidentes. Asimismo, se identifican factores determinantes que influyen en la capacidad de respuesta y recuperación de las organizaciones. El estudio aporta un conjunto de lineamientos estratégicos adaptados al contexto regional, orientados a fortalecer la resiliencia digital con recursos limitados. Se concluye que la madurez en ciberseguridad constituye un componente esencial para la sostenibilidad tecnológica y competitiva de las PYMEs en Iberoamérica.

Palabras-clave: Ciberseguridad; Resiliencia digital; Madurez tecnológica; Pequeñas y medianas empresas; Gestión de la información.

Cybersecurity Maturity and Digital Resilience in Ibero-American SMEs: Diagnosis and strategies challenges

Abstract: This article analyzes the level of cybersecurity maturity and digital resilience of Ibero-American small and medium-sized enterprises (SMEs), a sector particularly vulnerable to the rise of global cyberthreats. Using an exploratory-descriptive approach, we propose a diagnostic model based on the NIST Cybersecurity Framework, complemented by organizational management and security culture indicators. The results reveal significant gaps in the adoption of formal policies, staff training, and operational continuity in the event of incidents. Furthermore, determining factors that influence organizations' response and recovery capacity are identified. The study provides a set of strategic guidelines adapted to the regional context, aimed at strengthening digital resilience with limited resources. It concludes that cybersecurity maturity is an essential component for the technological and competitive sustainability of SMEs in Ibero-America.

Keywords: Cybersecurity; Digital Resilience; Technological Maturity; Small and Medium-Sized Enterprises; Information Management.

1. Introducción

En los últimos diez años, la rápida digitalización ha transformado la forma en que las pequeñas y medianas empresas (PYMEs) operan, producen y compiten. Las herramientas digitales han mejorado la eficiencia y el acceso a los mercados globales, pero también han incrementado la exposición a amenazas cibernéticas. En el entorno digital actual, las PYMEs de América Latina y España enfrentan riesgos cada vez más complejos, lo que convierte a la ciberseguridad en una cuestión estratégica para los negocios y no solo en un problema técnico. La Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) informaron en 2023 que el 80 % de las empresas latinoamericanas sufrió al menos un ciberataque en los últimos dos años, y que más del 60 % de los casos afectó a PYMEs (OEA & BID, 2023).

A diferencia de las grandes empresas, que cuentan con sistemas sólidos de ciberseguridad, las PYMEs suelen operar con presupuestos reducidos, capacidades técnicas limitadas y escaso conocimiento de las normativas en materia de seguridad digital. Esta situación resulta especialmente problemática si se considera que las PYMEs representan más del 95 % de las empresas en América Latina y España y generan aproximadamente el 67 % del empleo total (CEPAL, 2022). Diversos estudios señalan que el 58 % de las PYMEs latinoamericanas no dispone de planes formales de ciberseguridad y que solo el 25 % cuenta con capacidades de recuperación ante ataques, lo que incrementa el riesgo operativo y debilita la confianza de clientes y socios comerciales (Kaspersky, 2024).

La ciberseguridad comprende el conjunto de acciones, herramientas y normativas destinadas a proteger los sistemas de información y los activos digitales frente a ataques (NIST, 2022). En la actualidad, este concepto trasciende el ámbito puramente tecnológico e incorpora dimensiones organizacionales, culturales y humanas. De forma complementaria, la resiliencia digital se refiere a la capacidad de una organización para resistir, adaptarse y recuperarse de incidentes cibernéticos, garantizando la continuidad de sus operaciones (ENISA, 2023). Ambas dimensiones confluyen en el concepto de madurez en ciberseguridad, entendido como el grado en que las prácticas de seguridad están formalizadas, supervisadas y sujetas a procesos de mejora continua (Bada et al., 2021).

Para hacer frente al aumento de las amenazas digitales, se han desarrollado diversos modelos de madurez. El NIST Cybersecurity Framework (NIST CSF) es uno de los más utilizados y se estructura en las funciones de identificar, proteger, detectar, responder y recuperar. Otros enfoques, como el Cybersecurity Capability Maturity Model (C2M2) y la norma ISO/IEC 27001:2022, persiguen objetivos similares. No obstante, estos modelos fueron concebidos principalmente para organizaciones con elevados recursos tecnológicos y financieros, lo que limita su adecuación a las PYMEs de América Latina y España (Silva & Costa, 2023).

Los desafíos de la ciberseguridad en la región se ven agravados por deficiencias de infraestructura, debilidades en la gobernanza digital, escasa cooperación entre los sectores público y privado y una limitada disponibilidad de capital humano especializado.

La Estrategia Iberoamericana de Transformación Digital 2022–2025 reconoce que estas carencias reducen la competitividad regional y aumentan la dependencia tecnológica externa (SEGIB, 2022). Asimismo, la falta de una cultura preventiva y la percepción de la ciberseguridad como una prioridad secundaria por parte de la gestión empresarial constituyen obstáculos relevantes para la implementación de políticas efectivas (Gutiérrez & Hernández, 2021; Molina et al., 2023).

Desde una perspectiva operativa, las PYMEs tienden a priorizar la productividad de corto plazo, postergando las inversiones en ciberseguridad ante la dificultad de estimar sus beneficios. Como resultado, muchas operan en lo que el *ENISA Threat Landscape 2024* denomina una "zona de riesgo latente", caracterizada por niveles de protección insuficientes, ausencia de planes de contingencia, monitoreo limitado y escasa capacitación del personal. Entre las amenazas más frecuentes se encuentran los ataques de ransomware, el phishing avanzado, la filtración de datos, la explotación de vulnerabilidades en software desactualizado y los riesgos asociados a la cadena de suministro digital (ENISA, 2024).

Si bien la literatura reciente ha comenzado a vincular la ciberseguridad con el aprendizaje organizacional y la resiliencia estratégica (Teece, 2018; Radanliev et al., 2022), la investigación empírica sobre la madurez en ciberseguridad de las PYMEs en América Latina y España sigue siendo limitada. La mayoría de los estudios se concentra en Europa, Norteamérica o en grandes organizaciones, dejando a las PYMEs subrepresentadas (Hernández et al., 2021). Esta brecha limita el diseño de estrategias contextualizadas y debilita la efectividad de las políticas públicas.

Este estudio aborda dicha laguna mediante un análisis de la madurez en ciberseguridad y la resiliencia digital en PYMEs de América Latina y España. A partir de un enfoque metodológico mixto, basado en el NIST Cybersecurity Framework adaptado a las PYMEs, se analizan las prácticas de seguridad, las capacidades de respuesta ante incidentes y la cultura organizacional en relación con el riesgo digital.

El objetivo de la investigación es evaluar el nivel de madurez en ciberseguridad de las PYMEs latinoamericanas y españolas, identificar brechas clave y proponer lineamientos adecuados al contexto regional. En particular, se busca responder a las siguientes preguntas: (1) ¿Cuál es el nivel actual de preparación en ciberseguridad de las PYMEs? (2) ¿Qué factores internos y externos explican las debilidades en resiliencia digital? y (3) ¿Qué acciones pueden fortalecer la capacidad de respuesta y recuperación de las PYMEs?

El artículo se organiza de la siguiente manera. En primer lugar, se presenta la metodología de investigación y el modelo de madurez utilizado. A continuación, se exponen los resultados del análisis empírico, seguidos de una discusión que los vincula con la literatura reciente. Finalmente, se formulan recomendaciones estratégicas y se reflexiona sobre los desafíos futuros de la ciberseguridad en las PYMEs de América Latina y España.

2. Materiales y métodos

El presente estudio adoptó un enfoque mixto de carácter exploratorio-descriptivo y transversal, con el propósito de diagnosticar los niveles de madurez en ciberseguridad

y resiliencia digital en pequeñas y medianas empresas (PYMEs) de distintos países iberoamericanos. Se combinó el análisis cuantitativo mediante encuestas estructuradas con el análisis cualitativo a partir de entrevistas semiestructuradas, lo que permitió obtener una comprensión integral de las prácticas, vulnerabilidades y estrategias de respuesta adoptadas por las organizaciones ante amenazas digitales.

Este enfoque se seleccionó debido a que la ciberseguridad en las PYMEs es un fenómeno multidimensional, donde interactúan factores tecnológicos, humanos, organizacionales y regulatorios (ENISA, 2023; OEA & BID, 2022). El diseño transversal facilitó captar una fotografía representativa del estado actual de la madurez digital y de los mecanismos de resiliencia implementados en el ecosistema empresarial iberoamericano.

2.1. Diseño de la investigación

El estudio se estructuró en tres fases principales:

- Revisión documental: se realizó una revisión sistemática de literatura reciente (2020–2024) en bases de datos académicas como Scopus, Web of Science, Scielo y Google Scholar. Los términos de búsqueda incluyeron: “maturity model”, “cybersecurity in SMEs”, “digital resilience”, “Ibero-America”, y “risk management”. Esta fase permitió identificar marcos de referencia y estudios previos sobre niveles de madurez cibernética y resiliencia organizacional en PYMEs.
- Aplicación de encuesta estructurada: se diseñó un instrumento basado en el NIST Cybersecurity Framework (CSF) y en el modelo de madurez de la ENISA (2022). El cuestionario evaluó cinco funciones clave —Identify, Protect, Detect, Respond y Recover—, con escalas Likert de 1 a 5 para medir el grado de implementación de controles y prácticas de seguridad.
- Entrevistas cualitativas: se efectuaron entrevistas a 20 responsables de TI y gerentes generales de PYMEs en sectores manufacturero, tecnológico y de servicios de Argentina, Chile, España, México y Colombia. Las entrevistas, realizadas por videoconferencia, exploraron percepciones sobre riesgos, cultura organizacional y obstáculos a la adopción de políticas de ciberseguridad.

2.2. Población y muestra

La población objetivo estuvo conformada por PYMEs iberoamericanas con entre 10 y 250 empleados y operaciones digitales activas (e-commerce, gestión en la nube o servicios basados en TIC). La selección de un muestreo no probabilístico intencional se debió a que el estudio era exploratorio. También hubo dificultades para encontrar marcos muestrales completos y similares de pequeñas y medianas empresas (PYMEs) con capacidades digitales parecidas en Iberoamérica. En estudios diagnósticos y comparativos como este, el muestreo intencional es útil cuando se quiere analizar a fondo organizaciones que tienen riesgos cibernéticos y una gestión tecnológica básica (Patton, 2015; Hair et al., 2022).

El criterio de incluir empresas con al menos cinco años de actividad digital sirvió para confirmar que la madurez observada reflejaba prácticas establecidas y no procesos de digitalización recientes. La distribución por país buscó captar la variabilidad contextual

sin favorecer a ningún país en particular, lo que mejoró la capacidad de comparar el modelo en la región.

2.3. Procedimiento de recolección y análisis de datos

La recolección de datos se llevó a cabo entre abril y julio de 2024. Las encuestas fueron administradas en línea mediante formularios seguros con autenticación de usuario. Los datos cuantitativos se procesaron con SPSS v.28, aplicando análisis descriptivos, índices de madurez ponderados y comparaciones interregionales. El análisis cualitativo se realizó con NVivo 14, codificando las entrevistas en torno a tres categorías: cultura de seguridad, gestión de incidentes y aprendizaje organizacional.

Para evaluar la madurez en ciberseguridad, se aplicó un índice compuesto adaptado del modelo CMMI (Capability Maturity Model Integration), clasificando las empresas en cinco niveles: Inicial, Gestionado, Definido, Cuantitativamente Gestionado y Optimizado. La resiliencia digital se midió según la capacidad de recuperación operativa posterior a incidentes, siguiendo los lineamientos del Digital Operational Resilience Act (DORA, 2022).

Índice de madurez en ciberseguridad

El índice de madurez se creó con un modelo jerárquico de suma ponderada. Cada una de las cinco funciones del NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar) se midió con elementos específicos, basados en las prácticas recomendadas por NIST y ENISA. Los puntajes se estandarizaron en una escala de 0 a 100 y se sumaron con el mismo peso, ya que no había datos previos que justificaran darles pesos diferentes en las PYMEs iberoamericanas.

El puntaje total de madurez se calculó como el promedio ponderado de las cinco funciones y se ubicó en uno de los cinco niveles del modelo CMMI adaptado, usando puntos de corte teóricos definidos (0–20 Inicial; 21–40 Gestionado; 41–60 Definido; 61–80 Cuantitativamente Gestionado; 81–100). Esto aseguró que el índice fuera transparente, reproducible y consistente.

Además de los análisis descriptivos, se calcularon intervalos de confianza del 95 % para los puntajes promedio de madurez y resiliencia digital por país y sector, para estimar la precisión de los resultados. Se reportaron tamaños del para evaluar la magnitud de las diferencias entre grupos, evitando basarse solo en la estadística.

Se estimaron modelos de regresión multivariada para ver la relación entre la madurez en ciberseguridad (variable dependiente) y factores de la organización como tamaño, sector, país, políticas de seguridad formales y capacitación del personal (variables independientes). Estos modelos ayudaron a controlar factores externos y aportaron datos más sólidos sobre qué determina la madurez digital en PYMEs iberoamericanas.

Modelo de madurez iberoamericano propuesto

El modelo de madurez iberoamericano propuesto es un marco que une estándares internacionales (NIST CSF, ENISA y CMMI) con características de Iberoamérica. Funciona con una progresión secuencial, donde cada nivel de madurez implica

incorporar controles técnicos y desarrollar capacidades organizacionales, culturales y de aprendizaje.

2.4. Consideraciones éticas y validez

El estudio cumplió con los principios éticos de confidencialidad y consentimiento informado. Se garantizó el anonimato de las empresas participantes y se utilizó la información únicamente con fines académicos. Para asegurar la validez y fiabilidad, el cuestionario fue sometido a una prueba piloto en 10 empresas, alcanzando un coeficiente de consistencia interna $\alpha = 0{,}86$ (alta confiabilidad).

2.5. Limitaciones del estudio

Los resultados deben interpretarse como indicativos de tendencias observadas en PYMEs de los países analizados y no como representativos del conjunto de PYMEs iberoamericanas.

Entre las principales limitaciones se reconoce la disparidad en los niveles de digitalización entre países y sectores, así como la posible autoselección de empresas más sensibilizadas con el tema de ciberseguridad. No obstante, la combinación metodológica y el enfoque comparativo proporcionan una base sólida para la interpretación de resultados y la elaboración de políticas de fortalecimiento digital para el tejido empresarial iberoamericano.

3. Resultados

Los resultados obtenidos permiten caracterizar el estado actual de la madurez en ciberseguridad y resiliencia digital de las PYMEs iberoamericanas, así como identificar los factores que condicionan su desarrollo y las brechas existentes entre países y sectores. En términos generales, los hallazgos muestran que las PYMEs de la región presentan niveles medios o bajos de madurez, con un predominio de enfoques reactivos frente a las amenazas digitales.

3.1. Nivel de madurez en ciberseguridad

A partir del modelo de referencia del NIST Cybersecurity Framework (CSF), se calcularon los niveles promedio de madurez en las cinco funciones clave. La Tabla 1 resume los resultados agregados para los cinco países analizados.

Función NIST	Argentina	Chile	México	Colombia	España	Promedio regional
Identify	2,8	3,0	2,7	2,6	3,4	2,9
Protect	2,6	2,9	2,5	2,4	3,2	2,7
Detect	2,3	2,7	2,2	2,1	3,0	2,5
Respond	2,1	2,5	2,3	2,0	2,8	2,3
Recover	2,4	2,8	2,5	2,2	3,1	2,6

Tabla 1 – Niveles promedio de madurez en ciberseguridad por función y país (escala 1–5)

Los resultados evidencian que España presenta el mayor nivel promedio de madurez (3,1), seguido por Chile (2,8), mientras que Colombia y México registran los niveles más bajos (2,3–2,4). Las funciones más desarrolladas corresponden a Identify y Protect, mientras que Respond y Detect muestran las mayores debilidades, reflejando una tendencia a la reacción tardía ante incidentes más que a la prevención proactiva.

En el análisis por sector, las PYMEs tecnológicas y de servicios financieros alcanzaron los niveles más altos de madurez (promedios de 3,2 y 3,0 respectivamente), en contraste con las empresas manufactureras y de comercio minorista, que no superan el 2,5. Estos datos concuerdan con estudios previos que señalan que las organizaciones más digitalizadas tienden a adoptar mejores prácticas de seguridad (ENISA, 2023; OEA & BID, 2022).

3.2. Factores que influyen en la madurez

El análisis de regresión simple reveló una correlación positiva significativa (r = 0,67, p; 0,01) entre la madurez cibernética y la existencia de políticas formales de gestión de riesgos digitales. Asimismo, se encontró una asociación moderada (r = 0,54, p ; 0,05) entre el nivel de madurez y la formación del personal en seguridad de la información.

Las entrevistas cualitativas destacaron tres obstáculos principales:

1. Limitaciones presupuestarias, que dificultan la inversión en herramientas y auditorías.
2. Escasa cultura organizacional orientada a la ciberseguridad, percibida como un asunto técnico y no estratégico.
3. Dependencia de proveedores externos sin criterios homogéneos de seguridad.

Un gerente de TI de una PYME chilena señaló: *“La seguridad se atiende cuando ocurre un incidente; antes de eso, no se le asigna prioridad”*. Este patrón se repitió en la mayoría de las entrevistas, reforzando la necesidad de un enfoque sistémico.

3.3. Resiliencia digital y recuperación operativa

En cuanto a resiliencia digital, el 62% de las empresas indicó haber sufrido al menos un incidente de seguridad en los últimos 24 meses. Sin embargo, solo el 27% disponía de un plan formal de continuidad de negocio y un 19% había realizado simulacros de recuperación.

Las organizaciones españolas y chilenas mostraron mayor preparación, con tiempos medios de recuperación (MTTR) inferiores a 24 horas, mientras que en México y Colombia superaron las 48 horas. Estos resultados reflejan una brecha significativa en la capacidad de respuesta y recuperación, lo cual impacta directamente en la sostenibilidad del negocio y la confianza de los clientes (BID, 2023).

3.4. Comparación con estudios previos

Para situar los resultados en un contexto más amplio, la Tabla 2 resume los principales aportes de investigaciones relevantes sobre ciberseguridad en PYMEs publicadas entre 2015 y 2024.

Como se observa, la literatura muestra una evolución gradual desde el reconocimiento de la vulnerabilidad estructural (Cisco, 2015) hasta la incorporación de la resiliencia como pilar estratégico (ENISA, 2023). Este estudio amplía esa línea al ofrecer un diagnóstico empírico comparativo que integra las dimensiones técnicas y culturales de la seguridad digital.

Autor(es)	Año	Alcance	Principales hallazgos	Relevancia para este estudio
Cisco & IDC	2015	Global	Las PYMEs representan el 43% de los objetivos de ciberataques.	Evidencia temprana de vulnerabilidad estructural.
OEA & Symantec	2016	América Latina	Falta de políticas regionales coordinadas en ciberseguridad.	Base para políticas públicas actuales.
ENISA	2018	Europa	Modelos de madurez adaptados al tamaño de las empresas.	Referencia para escalas de medición.
CISA	2020	EE. UU.	Enfoque en resiliencia digital post-pandemia.	Inspiró el componente de recuperación.
OEA & BID	2022	Iberoamérica	Brechas formativas y baja adopción del enfoque preventivo.	Comparación directa con resultados actuales.
ENISA	2023	Europa	Promueve cultura de ciberseguridad como factor clave de resiliencia.	Refuerza la importancia del componente humano.
Torres & Calderón	2024	Chile y Colombia	Niveles medios-bajos de madurez tecnológica en PYMEs.	Corroboración empírica de los hallazgos.

Tabla 2 – Principales estudios sobre ciberseguridad y resiliencia digital en PYMEs (2015–2024)

4. Discusión

Los resultados obtenidos indican que la madurez en ciberseguridad y la resiliencia digital en las PYMEs iberoamericanas siguen siendo dimensiones en construcción, caracterizadas por estrategias fragmentadas y dependientes del contexto económico y regulatorio. Esta situación coincide con tendencias globales descritas en la literatura de la última década, que señalan la creciente brecha entre la sofisticación tecnológica de las amenazas y la capacidad de respuesta de las organizaciones de menor tamaño (ENISA, 2018; OEA & BID, 2022).

4.1. Interpretación general de los hallazgos

La evidencia empírica sugiere que, si bien la digitalización ha avanzado rápidamente en la región, la gestión del riesgo cibernético no ha evolucionado al mismo ritmo. Las funciones del marco NIST mejor valoradas —Identify y Protect— corresponden a acciones reactivas o de cumplimiento mínimo, mientras que las más débiles —

Respond y Recover— demandan una planificación estratégica que pocas empresas han institucionalizado. Este patrón coincide con lo identificado por OEA & Symantec (2016) y Torres & Calderón (2024), quienes advierten que el enfoque predominante en América Latina continúa siendo reactivo y centrado en la corrección posterior al incidente.

Los resultados también sugieren que la madurez cibernética no depende exclusivamente de la infraestructura tecnológica, sino de factores organizacionales, culturales y formativos, en línea con la visión de Von Solms & Van Niekerk (2018) sobre la necesidad de integrar la cultura de seguridad dentro del comportamiento corporativo. Esta relación se refleja en la correlación positiva entre la formación del personal y el nivel de madurez alcanzado.

4.2. Comparación con la literatura internacional

El panorama iberoamericano guarda similitudes con experiencias internacionales en cuanto a las dificultades de las PYMEs para desarrollar ecosistemas digitales resilientes. Sin embargo, existen diferencias marcadas en la disponibilidad de políticas públicas y programas de apoyo.

La Tabla 3 sintetiza los aportes más relevantes de autores y organismos internacionales en el período 2015–2024, que permiten contextualizar y contrastar los resultados obtenidos.

Autor(es) / Fuente	Año	Contexto geográfico	Aporte principal	Coincidencia con este estudio
Cisco & IDC	2015	Global	Identifican que el 43 % de los ciberataques se dirigen a PYMEs.	Confirma la exposición estructural del sector.
ENISA	2018	Europa	Propone modelos de madurez ajustados al tamaño de empresa.	Base metodológica del índice aplicado.
Von Solms & Van Niekerk	2018	Sudáfrica	Introducen el concepto de cultura de ciberseguridad organizacional.	Refuerza el vínculo entre cultura y resiliencia.
CISA	2020	EE. UU.	Define lineamientos de resiliencia digital post-COVID-19.	Apoya la incorporación de indicadores de recuperación.
OEA & BID	2022	Iberoamérica	Diagnostican brechas formativas y bajo nivel de preparación.	Coincide plenamente con los resultados regionales.
ENISA	2023	Europa	Destaca la formación continua y el liderazgo como ejes de resiliencia.	Reflejado en la correlación hallada entre formación y madurez.
Torres & Calderón	2024	Chile-Colombia	Reportan niveles medios-bajos de madurez digital.	Confirma los patrones detectados en este estudio.

Tabla 3 – Estudios internacionales relevantes sobre ciberseguridad y resiliencia en PYMEs (2015–2024)

Estos antecedentes muestran una evolución conceptual hacia la integración de la cultura organizacional y la resiliencia digital como dimensiones críticas de la seguridad. La presente investigación amplía esa tendencia al ofrecer datos empíricos comparativos de cinco países, algo escasamente documentado en la región.

4.3. Factores estructurales y culturales

El análisis comparativo sugiere que los países con políticas nacionales de ciberseguridad consolidadas —como España y Chile— presentan mejores indicadores de madurez. Este hallazgo respalda la hipótesis de González & Ramos (2021), quienes sostienen que la presencia de marcos regulatorios estables y programas estatales de capacitación correlaciona con mayores niveles de preparación digital.

Por el contrario, en países donde las políticas son incipientes o desarticuladas, las PYMEs dependen casi exclusivamente de su capacidad interna, lo que genera disparidades incluso dentro de un mismo sector. La falta de incentivos fiscales o de certificaciones adaptadas al tamaño empresarial limita la adopción de medidas preventivas sostenibles.

A nivel organizacional, se observa que la percepción de la ciberseguridad como un gasto y no como una inversión estratégica continúa siendo una barrera, tal como señalan Calder & Moody (2019). En las entrevistas, la mayoría de los gerentes asoció la seguridad digital a la tecnología de hardware, sin reconocer su dimensión humana o de procesos.

Dimensión	Factor determinante	Evidencia empírica	Referencia
Organizacional	Liderazgo comprometido con la seguridad	Correlación r = 0,61 con madurez	ENISA (2023)
Cultural	Conciencia del personal sobre riesgos digitales	68 % de las PYMEs sin capacitación anual	Torres & Calderón (2024)
Estructural	Disponibilidad presupuestaria	72 % reporta limitaciones	BID (2023)
Institucional	Existencia de marco normativo nacional	Mejores índices en España y Chile	González & Ramos (2021)

Tabla 4 – Factores internos y externos que influyen en la madurez cibernética

La evidencia demuestra que la madurez tecnológica no garantiza resiliencia digital si no se acompaña de liderazgo directivo, cultura preventiva y políticas públicas coherentes.

4.4. Hacia un modelo iberoamericano de madurez y resiliencia

Los resultados y la literatura convergen en la necesidad de desarrollar un modelo regional de madurez cibernética que considere la heterogeneidad económica y cultural de las PYMEs iberoamericanas. Tal enfoque debería combinar tres niveles:

- Técnico, basado en los marcos NIST y ENISA.
- Organizacional, que incorpore prácticas de gestión del conocimiento y cultura de seguridad.
- Ecosistémico, que articule políticas estatales, cámaras empresarias y universidades.

Nivel	Características principales	Enfoque dominante
Inicial	Ausencia de políticas formales; acciones reactivas.	Técnico-correctivo.
Gestionado	Procedimientos básicos y responsable designado.	Cumplimiento normativo.
Definido	Procesos documentados y capacitación regular.	Gestión integral del riesgo.
Cuantitativamente gestionado	Indicadores de desempeño y monitoreo continuo.	Prevención sistemática.
Optimizado	Cultura de resiliencia y mejora continua.	Estrategia corporativa.

Tabla 5 – Propuesta sintética de niveles de madurez adaptados al contexto iberoamericano

Este modelo, derivado de los hallazgos empíricos y de la revisión de marcos internacionales, busca ofrecer una herramienta adaptable a la realidad de las PYMEs de la región, facilitando diagnósticos periódicos y la implementación gradual de capacidades de ciberresiliencia.

El modelo propuesto tiene un carácter exploratorio y heurístico, y requiere validación empírica adicional en un mayor número de países y sectores.

4.5. Implicaciones teóricas y prácticas

Desde el punto de vista teórico, este estudio refuerza la necesidad de integrar la teoría de capacidades dinámicas (Teece, 2018) en el análisis de la ciberseguridad organizacional, entendiendo la resiliencia como una competencia estratégica que se aprende y evoluciona. En el plano práctico, aporta evidencias útiles para diseñar políticas públicas de apoyo, programas de certificación adaptados al tamaño empresarial y estrategias formativas sectoriales.

La madurez en ciberseguridad deja de ser un atributo técnico para convertirse en un indicador de sostenibilidad empresarial, estrechamente vinculado con la continuidad operativa y la confianza digital. Los resultados sugieren que fortalecer la resiliencia de las PYMEs no solo mejora su protección, sino que también incrementa su competitividad y su capacidad de integrarse en cadenas globales de valor digital.

5. Conclusiones

Este artículo ha demostrado que la madurez en ciberseguridad y la resiliencia digital constituyen factores estratégicos determinantes para la sostenibilidad de las PYMEs iberoamericanas en un entorno de creciente digitalización y riesgo. A partir del diagnóstico realizado en cinco países de la región, se evidenció que, aunque la adopción tecnológica ha avanzado de manera significativa, la gestión de la ciberseguridad continúa anclada en enfoques reactivos, dependientes de la infraestructura técnica y poco integrados en la cultura organizacional.

Los resultados han permitido confirmar el cumplimiento de los objetivos de la investigación: (1) caracterizar el nivel de madurez en ciberseguridad de las PYMEs analizadas de los distintos países a partir del modelo NIST, (2) identificar los factores estructurales, culturales y de liderazgo que condicionan la resiliencia digital, y (3) establecer lineamientos estratégicos para la evolución hacia modelos más integrales y sostenibles de gestión del riesgo digital. La evidencia empírica recogida, junto con la revisión de la literatura internacional, confirma que la madurez cibernética no puede comprenderse sin integrar dimensiones humanas, cognitivas y culturales en el análisis.

En cuanto a la pregunta de investigación —¿cuál es el nivel de madurez en ciberseguridad y resiliencia digital de las PYMEs iberoamericanas, y qué factores estratégicos determinan su desarrollo?— los hallazgos indican que la región se encuentra, en las empresas analizadas, en un estadio medio-bajo de preparación. Las capacidades más desarrolladas se concentran en la identificación y protección, mientras que las relacionadas con la respuesta y recuperación ante incidentes muestran una clara debilidad. Estos resultados concuerdan con diagnósticos previos realizados por organismos como la OEA y el BID, y evidencian una brecha creciente entre el ritmo de digitalización y la madurez en la gestión de riesgos tecnológicos.

Asimismo, se ha comprobado que las variables más influyentes en la madurez organizacional son el liderazgo comprometido, la capacitación continua y la existencia de políticas públicas de apoyo. Las empresas que incorporan la ciberseguridad como parte de su estrategia de negocio y que promueven una cultura de conciencia digital alcanzan niveles significativamente más altos de resiliencia. Por el contrario, aquellas que perciben la seguridad como un gasto operativo presentan respuestas reactivas, vulnerabilidades recurrentes y menor capacidad de recuperación post-incidente.

Esta investigación también aporta implicaciones prácticas relevantes. En primer lugar, resalta la necesidad de diseñar modelos de madurez adaptados al contexto iberoamericano, que combinen estándares internacionales (NIST, ENISA) con particularidades culturales y económicas de la región. En segundo lugar, sugiere la urgencia de articular políticas públicas, cámaras empresariales y universidades para desarrollar programas de formación y certificación que fortalezcan el capital humano en ciberseguridad. En tercer lugar, plantea la conveniencia de promover ecosistemas colaborativos de intercambio de información sobre incidentes, que incrementen la capacidad de respuesta sectorial.

Finalmente, este estudio contribuye a la literatura sobre gestión de la ciberseguridad al proponer una visión integral y evolutiva de la madurez digital, entendida no solo como un estado técnico, sino como una competencia dinámica y estratégica que se construye colectivamente. La resiliencia digital emerge, así, como un nuevo indicador de sostenibilidad empresarial, clave para la competitividad en mercados globalizados.

En consecuencia, se recomienda:

(1) consolidar un observatorio regional de madurez cibernética que monitoree avances y brechas;

(2) fomentar la formación continua de líderes y empleados en competencias digitales críticas;

(3) promover incentivos fiscales y certificaciones para las PYMEs que implementen buenas prácticas de seguridad;

y (4) realizar investigaciones longitudinales que evalúen la evolución de la madurez y la resiliencia digital en función de políticas nacionales y sectoriales.

El camino hacia una región digitalmente segura y resiliente no depende únicamente de la tecnología, sino de la capacidad colectiva para construir confianza, conocimiento y cultura de seguridad como ejes del desarrollo sostenible y competitivo iberoamericano.

Referencias

Banco Interamericano de Desarrollo. (2023). *Ciberseguridad: Avances y desafíos en América Latina y el Caribe*. BID. https://publications.iadb.org

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2021). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Calder, A., & Moody, S. (2019). *Information security risk management for ISO/IEC 27001*. IT Governance Publishing.

Cano, J. J. & Rocha, A. (2019). *Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (32). https://doi.org/10.17013/risti.32.0

Cisco & IDC. (2015). *Small business security: Threats are real, protection is critical*. Cisco Systems.

Comisión Económica para América Latina y el Caribe. (2022). *Transformación digital y seguridad de la información en las PYMEs de América Latina*. CEPAL. https://www.cepal.org

Cybersecurity and Infrastructure Security Agency. (2020). *Cyber resilience review*. U.S. Department of Homeland Security. https://www.cisa.gov

European Union Agency for Cybersecurity. (2018). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

European Union Agency for Cybersecurity. (2023). *National cybersecurity strategies evaluation framework*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

González, A., & Ramos, J. (2021). Políticas públicas y preparación digital en América Latina. *Revista de Administración Pública, 55*(2), 89–108.

Gutiérrez, L., & Hernández, P. (2021). Cultura organizacional y percepción del riesgo digital en PYMEs. *Revista Latinoamericana de Gestión, 14*(1), 33–49.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage.

Hernández, R., Fernández, C., & Baptista, P. (2021). *Metodología de la investigación* (7.ª ed.). McGraw-Hill.

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection*. International Organization for Standardization.

Kaspersky. (2024). *Cybersecurity risks for SMEs in Latin America*. Kaspersky Lab. https://www.kaspersky.com

Molina, F., Pérez, J., & Suárez, R. (2023). Madurez digital y gestión del riesgo en PYMEs iberoamericanas. *Revista Iberoamericana de Sistemas y Tecnologías de Información, 54*(1), 19–34.

National Institute of Standards and Technology. (2023). *Cybersecurity framework (Version 2.0)*. https://www.nist.gov/cyberframework

Organization of American States & Inter-American Development Bank. (2022). *Cybersecurity: Risks, progress, and the way forward in Latin America and the Caribbean*. OAS–IDB.

Organization of American States & Inter-American Development Bank. (2023). *Cybersecurity report 2023*. OAS–IDB.

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage.

Radanliev, P., De Roure, D., Nurse, J. R. C., & Burnap, P. (2022). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence. *Journal of Cybersecurity, 8*(1), 1–14. https://doi.org/10.1093/cybsec/tyac006

Sánchez-García, I. D., Rea-Guamán, A. M., San Feliu, T., & Calvo-Manzano, J. A. (2024). *Cybersecurity risk audit: Literature review, proposal, and application*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (53), 69–87. https://doi.org/10.17013/risti.53.69-87

Secretaría General Iberoamericana. (2022). *Estrategia iberoamericana de transformación digital 2022–2025*. Secretaría General Iberoamericana.

Silva, R., & Costa, E. (2023). Cybersecurity maturity models and SMEs: A systematic review. *Computers & Security, 122*, 102900. https://doi.org/10.1016/j.cose.2022.102900

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning, 51*(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007

Torres, J., & Calderón, M. (2024). Niveles de madurez digital en PYMEs de Chile y Colombia. *Revista Latinoamericana de Administración, 20*(2), 55–72.

Von Solms, R., & Van Niekerk, J. (2018). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. https://www.weforum.org/reports/global-cybersecurity-outlook-2024